*International Journal of Computer Science and Innovation*
Vol. 2015, no. 2, pp. 88-96
ISSN: 2458-6528

# A survey on cloud computing security issues

Yerneni Sushmitha, V Krishna Reddy, D Pavan Teja Reddy

Department of Computer Sciences and Engineering, K L University, Andhra Pradesh, India
Email: *Sushmitha4292@gmail.com*

***Abstract*** - Cloud computing is the process of delivering the resources through internet. In cloud computing resources can be utilized with efficient cost. When data is stored in cloud there should be standards and procedures to secure the information. Security in cloud is a major challenge as many threats and risk are associated with this computing model. This paper deals with the issues in cloud deployment models like public, private, community, hybrid clouds. Cloud computing provides mainly 3 cloud service models where each model have their own security issues.

***Keywords:*** *Cloud security, deployment models, service models.*

## I. INTRODUCTION

A new computing prototype cloud computing is a new delivery model which has grown rapidly in recent years. According to Nation's institute of standards and technology (NIST), "Cloud computing is usually a model for enabling Convenient, on-demand network use of a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that may be rapidly provisioned and released with minimal management effort or vendor interaction". The cloud computing model composed with five essential characteristics [1].

The cloud computing components comprise front end, backend and communication. The front end is computer interface includes client's network, through web browser user can access the applications. The communication channel acts as the mediator between front end and back end. The back end is cloud itself consists of data storage devices, servers [4]. Data and applications are the assets to deploy in cloud. Identify the suitable deployment model and appropriate cloud service model to maintain the data [2]. This paper deals with back end layer. In every aspect the security is main concern .To shift to the cloud computing there are many data security and privacy risks. Security stance first as the greater challenge issues in cloud computing [3].

Nonprofit organization like Cloud security Alliances (CSA) is solution provider.CSA discuss on best process and future approach for securing information in cloud [19].

The Open Web Application Security Project (OWASP) charitable, nonprofit management concentrates on securing the software and its improvements. Discussions on software security risks are held and it involves web application security also [20].

The open global communities Open Grid Forum (OGF) focus on evolutions and adoptions on distributed computing like cloud, grid. It accomplishes its work through open forums, open standards [21].

This paper is organized as follows: Section 2 illustrate about cloud computing security. Section 3 illustrate about security issues posed by Deployment models. Section 4 illustrate about security issues posed by cloud service models. Section 5 conclusions this survey.

## II. CLOUD SECURITY

When the sensitive data is stored in cloud the main concerns are how it is secured, what are the rules and procedures to protect the data. Customers when migrating to the cloud they trust the third party vender who ensures the requirements like confidentiality, authenticity and integrity of data. The building blocks of cloud security are :[5].

- ***Confidentiality:***
  The ability to access the protected data by the authorized users refers to confidentiality [6].Unauthorized access leads of data privacy risks and leakage of data.
- ***Authentication:***
  Authentication refers to identify the credentials of the individual and verify whether they are privileged users or not [23]. Now a days there are many approaches available like biometric scans, graphical passwords, 3Dpassword, third-party authentication.
- ***Integrity:***
  During the data transmission capability to the protect data from not being destroyed or manipulated by unauthorized persons refers to integrity [5].

## III. DEPLOYMENT MODELS

In cloud environment there are four deployment models based on NIST [1].

### *A. Public cloud*

This cloud infrastructure provides access to public [6]. Adopting public cloud environment have many risks as it is used by everyone and there are more security considerations.

1. ***Multi tenancy:***
   Sharing of same resources by many tenants who are not related to each other leads to multi tenancy. Multi tenancy has its own benefits and several security threats. Both the cloud user and cloud infrastructure suffer with privacy vulnerabilities [7]. In the multitenant environment there are potential privacy risks, side-channel attacks to cloud user's information.
2. ***Malicious insiders:***
   Malicious insider is attacker who has access to the data in cloud data center, may be developer who develops code which is exploited by outsiders, may inject virus to the system etc.
3. ***Access Control:***
   Access Control is a strategy allows or restricts the user to access the system. Attempting to access the data by the unauthorized users can also be identified by this mechanism. In this process various steps are involved like identification, authentication and authorization [22]. User need to know how many can view your data? How many are having privileged access to the data? Can private keys be shared among multiple tenants? For privileged users what type of authentication is required? All the above information is need to be known to the user for the assurance of data protection by cloud service provider.
4. ***Virtual Exploits:***
   Cloud customer does not have the knowledge about what type of virtualization software the vender is using. Customer need to question about what version the vender is using? Patches in the virtualization is done by whom and when? Who are monitoring ,logging the each virtualization host and guest?

There are many virtual exploits such as guest to host, guest to guest, server host only, host to server which are unknown risk models not known by people.

### B. Private cloud

Because of many security issues in public cloud many firms migrate to private cloud deployment model [8]. This cloud infrastructure is efficiently owned by one organization [5]. Underlying hardware can have more control in private cloud than in public cloud because of its multi tenancy environment, to meet the organization's functional need private cloud affords better customization of the infrastructure. But in private cloud there are some security considerations:

#### 1. Defining responsibilities:

In this deployment model operational security changes from hands i.e. from one group to other or the cloud vendor. So, who is responsible for what must be out lined. Different policies and set of stakes are managed by different departments, users and domains. To avoid data leakage care must be taken when responsibility changes from hands.

#### 2. Elastic and changing perimeters:

The private cloud infrastructure is elastic i.e. delivery of resources is done on demand from pool of resources. Scaling out happens when required and security needs to be maintained for the changing perimeters also [9].

#### 3. Ineffective device-specific controls:

Virtual machines are not bound to specific hardware. So there is no device specific controls like traditional IT. Intelligent and adaptive security policies need to be initiated based on physical hardware [9].

### C. Community cloud

For multiple organizations this cloud infrastructure functions with a set of shared cooperatives and domain specific concerns [5]. The cloud environment is managed by any third party vendors or hosted by the organizations [6]. Community cloud can be either onsite or offsite [11].
Community clouds are used in healthcare, public sector and media.

In multitenant environment like community cloud, it reduces the costs of private cloud and abolish public cloud security threats [11].Below techniques and processes are to be followed:

#### 1. Identity management:

Identity management in community cloud involves in accessing the data by whom, when as well as where and how are monitored by service providers. Identity management needs supervising, enforcement, and provisioning. Auditing, accounting and forensics tools are required for supervising. In enforcement, access privileged is determined to the user and devices according to the policy. Authorizing and controlling network access to network devices using ACLs, VLANs and other mechanisms are involved in provisioning [10].

#### 2. Data protection and Integrity:

With high utilization and greater density the goal of cloud computing is to secure the data. Without affecting data integrity refined software need to be provided by cloud vendor for hardware breakdown. It is highly critical in virtualization for network and storage resources [10].

#### 3. Data governance:

Cloud providers who are responsible for stewards of data in multitenant environment need mandatory certification and regulations. Around the data lifecycle from creation to disposition governance polices need to be established by cloud service providers. Related to data governance cloud service providers need to set up platforms and systems to support regulations [10].

### D. *Hybrid cloud*

This infrastructure combines two or more clouds [12]. By allowing intercommunication between the cloud models the hybrid cloud remain unique entities and bound together.

In hybrid cloud due to separation of resources into multiple clouds the complexity of software and configuration increases while migrating resources of an enterprise. Apart from this there are many security complexities during communication between the clouds. Firewalls are provided to protect from outsider intrusions. There are possible threats to the enterprise data.

#### *1. Lack of data redundancy:*

In hybrid cloud environment lack of redundancy may become a security risk when copies of data are not distributed across data centers. There is a risk of data failure when running your application in single data center to another. Using multiple data centers from single cloud provider mitigates risks and save cost effectively.

#### *2. Security management:*

There are security requirements like identity management, authentication, and authorization for both public and private cloud [23]. Integrate these protocols, since both clouds can synchronize the data security. By using IMS, single service can be provided for systems running in either cloud.

#### *3. Compliance:*

In hybrid cloud environment maintaining and demonstrating compliance can be more difficult. In hybrid cloud ensure the moving data between private and public [13] is protected. Ensure prevention of data leakage from private cloud to less secured public cloud.

#### *4. Poorly Constructed SLAs :*

In service level agreement Public cloud can consistently meet expectations, but private cloud may not. Based on two clouds create SLAs on expectations of insignificant one, possibly private cloud. While integrating both clouds there may be potential risks that could disrupt service. If in private cloud the confidential and sensitive data is on - premise then SLA should reflect the limits in public cloud.

## IV. CLOUD SERVICE DELIVERY MODELS

In cloud computing cloud service delivery models are in classified into three services [1].

**Table 1.** *Services managed by cloud delivery models*

| **Delivery models** | **Managed by users** | **Managed by cloud providers** |
|---|---|---|
| Software as a service | Nothing | Networking , Storage, Server HW, Virtualization, Servers, Databases, Security & integration, Runtimes, Applications |
| Platform as a service | Applications | Networking , Storage, Server HW, Virtualization, Servers, Databases, Security & integration, Runtimes |
| Infrastructure as a service | Servers , Databases , Security & integration, Runtimes, Applications. | Virtualization, Server HW, Storage, Networking. |

## A. *Software as a service*

In this SaaS the software is delivered to the customer as service. From various client devices the applications are accessible over web browser. The underlying infrastructure network, server, storage, operating system are not managed or controlled by customer [5].

### 1. *Security issues in SaaS:*

SaaS is the dominant delivery model now days. With this SaaS model there are many concerns like application vulnerabilities, data breaches which lead to legal and financial liabilities. There should be fine grained authorization techniques for access control and encryption techniques for data security [14]. Network security is maintained by network layer which provides powerful protection against packet sniffing, port scanning, Man-in-Middle attacks, Ip spoofing. During SaaS development process the security elements considered are data access, data confidentiality, data integrity, availability, data breaches and data segregation [14].

A brief listing of the security considerations (by OWASP) that SaaS offering should address:

- Injecting malignant commands into OS, SQL, LDAP.
- Ruin session and authentication management.
- Not restricting access to URL.
- Referring to direct objects which are not secure.
- Redirects and forwards are not validated properly.
- Cross-site scripting and request forgery.
- Inadequate transport layer security.
- Unassertive cryptographic storage.
- Improper security configurations.

#### *1.1 Limitations to replicate the organization in the cloud:*

Cloud service provider must create thousands of mirror users on cloud if they potentially have thousands of employees. There is a duct on IT help desk assets and potential security threats when users have multiple passwords.

In any large organization leveraging applications with multiple passwords, there are risks and costs issues. For example, it is very costly to provide new password and access to cloud services for each individual user. Extra care is taken by IT Service department if new password is reset by the user for SaaS service when he forgot the password.

#### *1.2 Protect the API Keys:*

Using simple REST web services interface many cloud services are accessed known as APIs. Organizations access the cloud providers using API keys. For example, if an organization is using a SaaS contribution, it will generally be granted by an API Keys. The security of these keys is very essential. If the keys were stolen then an attacker can acquire control over the confidential data.

#### *1.3 Backup and recovery:*

Cloud service provider should maintain regular backups by using snapshots and have faster recovery techniques when disaster occurs. Sensitive information is protected by using strong encryption schemes for backup data to prevent accidental leakage. Unauthorized parties cannot access the data when data and backups are separately encrypted.

### B. *Platform as a service*

In this PaaS the cloud vender provides the platform to develop and deploy applications [5]. By using a PaaS development tool, user can install and build server environment and run an application which can reduce complexity and cost [24].

#### 1. *Security issues in PaaS:*

PaaS security can be done in 2 ways Firstly security of the PaaS platform itself provided by cloud service provider and secondly security of the deployed customer application on PaaS platform.

#### *1.1 Data location*:

PaaS provides storage capacity for resultant output or files. The actual platform is as a group of clustered hosts not a single host. The data location cannot be on a specific host. Instead of many locations single data location is easier to protect. PaaS minimizes the cost by giving development tools for software buildup. In this environment performance is achieved through duplication of data which provides high availability of data for users and developers. As the exact location is not known leads to security difficulties.

#### *1.2 Privileged access:*

To fix a problem in the code developers use built-in-debug. This permits access for data and memory location and modify values to test various cases. This tool offers privileged access not only for developers but also hackers. Programmers request full access to work in a privileged environment even though it is not necessary. This is guarantee not safest and best way to solve the problem.

#### *1.3 Distributed system:*

In PaaS environment file systems are highly distributed. Hadoop distributed file systems (HDFS) are most used for implementations. The Cloud service provider owns the cluster of namespaces/name nodes independently managed by HDFS. Attackers give various inputs to default ports in order to cause failures or Dos (Denial of service) [24]. There may be potential attack vectors for other ports which are used for management and operations. Client is liable to verify the security requirements, but cloud service provider need to provide the necessary security.

Always Physical security, network security and underlying hardware are managed by cloud service provider. Before signing the agreement customer need know about

- Whether Cameras are used to monitor?
- Do Systems have restricted access?
- For remote administrative tasks is two-factor authentication required?
- Whether Firewalls are arranged?
- Is your hypervisor common? If yes then with whom?
- Are the events logged?

Additionally, know whether cloud service provider qualified any certifications and have done assessments in cloud security.

### C. *Infrastructure as a service*

In IaaS model the cloud service provider provides the storage, server and network resources [5]. Cloud service provider manages the cloud infrastructure and host environment. Customer has the capability to provision network, storage and can deploy and run operating systems and applications [24].

### 1. *Security issues in IaaS:*

Virtualization is a technique where polled resources can be access in cloud computing environment [15] .To protect cloud area encompassment security capabilities are limited in virtualization technique [16]. Virtualization is the big security burden in IaaS. Security liabilities are there for both customer and cloud service provider ,both have different aspects to control. Data, applications, operating system are controlled by customer [5].Cloud service provider is responsible for virtualization security, physical security, environmental security [14].

***Containerization:*** Effective portability of applications is achieved by Container. Operating system level virtualization is also known as Containerization. Instead of one instance(container), multiple isolated user space instances are allowed by operating system kernel. It is more efficient than full hardware virtualization as containers share a single operating system kernel. Here, less security isolations are provided by containers than hardware virtualization. If containers provide more isolation it is better than a simple multiuser shared server. Fundamentally container based systems have much larger stack surface[18].

In virtual cloud infrastructure security risks can be divided into three categories [17]:

#### *1.1 Hypervisor Attacks:*

To gain control over complete infrastructure hackers consider hypervisor. If hypervisor is attacked he can have great control on installed VM, operating systems and running applications. Hyper jacking, BLUEPILL are popular attacks.

#### *1.2 vSwitch Attacks:*

This is similar to layer2 physical switch attack. These attacks include vSwitch configurations, trust zones, VLANs and ARP tables

#### *1.3 Virtual Machine Attacks:*

VM's may be offline or active they can be attacked. Cloud servers have tens of VMs. As VMs share the same hardware and software resources, if one VM is attacked then the other VMs have the possibility to be attacked. Therefore, increases the attack surface and risk of VM -to -hypervisor and VM-to-VM compromises [23]. When physical server is offline there will be no attacks. But when VM is offline still it is a image file. So there is possibility of patching and malware infections.

There are few security solutions:

- In Virtualization-Aware Security Solutions, dedicated and privileged VM(Sec VM)(security software )is deployed to secure the hypervisor and other VMs installed in same physical server. To get a look over VM from the hypervisor and to observer and monitor the VMs from outside, a VM SecVM is maintained. SecVM utilizes virtual machine introspection. It is harder for hacker to detect the security software installed [17].
- Micro Hypervisors are developed with the specialized micro kernel to secure the hypervisor. To shrink the most critical attack surface in hypervisor this approach is followed [17].
- In Hypervisor-Level Protection approach, the hypervisor need to be maintained more robust, as it secure the hypervisor itself. Page level protection techniques and memory management technique are used to protect and secure the hypervisor. To intensify trust and secure the operating platform powerful features like isolation enforcement, I/o memory management, multi-queue networks are provided by Intel and AMD [17].

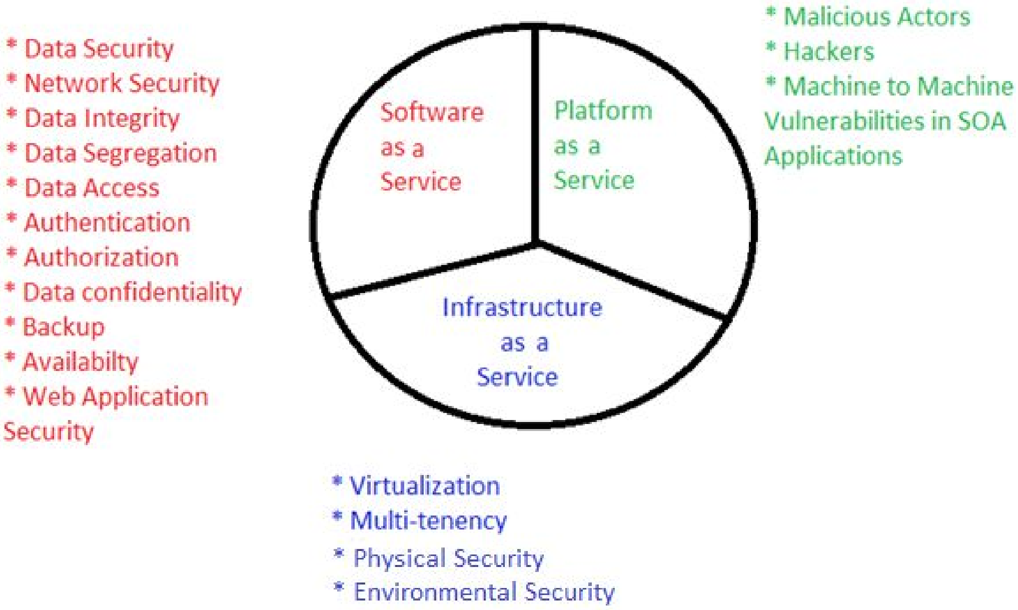

**Figure 1.** *Security issues in SaaS, PaaS, IaaS*

## V. CONCLUSION

In this paper security concerns are discussed in each stage of cloud computing. Security as service model will lead the future as it provides instructions to organizations by classifying different types of security as services. Adoption of cloud computing has rapidly increased because of its efficiency of cost and flexibility. Customized security mechanisms need to be introduced to mitigate the risks and attacks. Future work can be implemented on front end security issues.

## REFERENCES

[1] MEEL, P. et GRANCE, Timothy. The nist definition of cloud computing (draft).*National Institute of Standards and Technology, Gaithersburg*, 2011.

[2] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

[3] SO, Kuyoro. Cloud computing security issues and challenges. *International Journal of Computer Networks*, 2011, vol. 3, no 5.

[4] PATIL, Pradip. Cloud Security Issues. *Journal of Information Engineering and Applications*, 2015, vol. 5, no 1, p. 31-34.

[5] BALASUBRAMANIAN, V. et MALA T. A Review On Various Data Security Issues In Cloud Computing Environment And Its Solutions. *ARPN Journal of Engineering and Applied Sciences*. 2015, vol. 10, no. 2.

[6] ZISSIS, Dimitrios et LEKKAS, Dimitrios. Addressing cloud computing security issues. *Future Generation computer systems*, 2012, vol. 28, no 3, p. 583-592.

[7] REN, Kui, WANG, Cong, et WANG, Qian. Security challenges for the public cloud. *IEEE Internet Computing*, 2012, no 1, p. 69-73.

[8] SumitGoyal Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review I.J. *Computer Network and Information Security*, 2014, 3, 20-29 Published Online February 2014 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2014.03.03

[9] SUBRAMANIAN Krishnan. Analyst & Researcher. Private Clouds. *A whitepaper* sponsored by Trend Micro Inc.

[10] Securing Government Private and Community Clouds (http://www.cisco.com/web/strategy/docs/gov/c45-617006_aag.pdf)(Accessed on: December 15, 2015).

[11] FERNANDES, Diogo AB, SOARES, Liliana FB, GOMES, João V., *et al.*Security issues in cloud environments: a survey. *International Journal of Information Security*, 2014, vol. 13, no 2, p. 113-170.

[12] KOUSHIK Annapureddy. School of Science and Technology. Security Challenges in Hybrid Cloud Infrastructures Aalto University, T-110.5290 *Seminar on Network Security* Fall 2010

[13] SEN Jaydip. Innovation Labs Security and Privacy Issues in Cloud Computing , *Tata Consultancy Services* Ltd., Kolkata, INDIA

[14] SUBASHINI, Subashini et KAVITHA, V. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 2011, vol. 34, no 1, p. 1-11.

[15] KUMAR, Sarvesh, SINGH, Suraj Pal, SINGH, Ashwanee Kumar, *et al.*Virtualization, The Great thing and Issues in Cloud Computing. *International journal of Current Engineering and Technology*, 2013, vol. 3.

[16] SABAHI, Farzad. Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. *Int. Journal of Machine Learning and Computing*, 2012, vol. 2, no 1.

[17] KUMAR, A., SRINIVASULU, C., KUMAR, B. Sudeep, *et al.* Emphasis and emerging trends on virtualization of cloud infrastructure with security challenges. *International Journal of Computer Trends and technology (IJCTT), ISSN*, 2013, p. 2231-2803.

[18] WHEELER, David A. Cloud Security: Virtualization, Containers, and Related Issues.

[19] Cloud security alliance https://cloudsecurityalliance.org/(Accessed on: December 15, 2015)

[20] The Open Web Application Security Project https://www.owasp.org/index.php/Main_Page (Accessed on: December 15, 2015)

[21] Open grid forum https://www.ogf.org/ogf/doku.php (Accessed on: December 15, 2015).

[22] KHAN, Abdul Raouf. Access control in cloud computing environment. *ARPN Journal of Engineering and Applied Science*, 2012, vol. 7, no 5, p. 613-615.

[23] REDDY, V. Krishna et REDDY, L. S. S. Security architecture of cloud computing. *International Journal of Engineering Science and Technology*, 2011, vol. 3, no 9.

[24] REDDY, V. Krishna, RAO, B. Thirumala, et REDDY, L. S. S. Research issues in cloud computing. *Global Journal of Computer Science and Technology*, 2011, vol. 11, no 11.